Articoli e saggi

José Justo Megías Quirós

Vida privada y nuevas tecnologías

Sumario: 1. Hacia el reconocimiento constitucional de la vida privada. – 1.1. El derecho a la intimidad. – 1.2. El derecho al secreto de las comunicaciones. – 1.3. La libertad informática o autodeterminación informativa. – 2. Vulneraciones más generalizadas de la vida privada en la Sociedad de la Información. – 2.1. Riesgos derivados de la protección de los derechos de autor. – 2.2. Los riesgos de la privacidad en el ámbito laboral. – 3. Conclusión.

Carece de sentido el reconocimiento de derechos humanos y su positivación como derechos fundamentales en los textos internacionales y constitucionales si no tienen como fin primario asegurar la dignidad del ser humano y su libre desarrollo personal de acuerdo con su natural modo de ser ([1]). De nada serviría contar con un listado de derechos teóricos, derechos a los que reconoceríamos sobre el papel una importancia decisiva para vivir como personas, si no van acompañados de sus contornos, garantías, medios y mecanismos suficientes para hacerlos efectivos. Esto tiene especial trascendencia en el ámbito de la vida privada, pues nuestras opiniones y decisiones se forman en él antes de que tengan repercusión en el ámbito público, en nuestras relaciones con los demás. Cada ser humano tiene derecho a ser quien desea ser – sin salirse de lo humano –, a realizar su proyecto de vida – sin desconocer que convive con los demás – y a elegir las metas que mayor satisfacción le reporten como persona; para ello tendrá que tomar una serie de decisiones con plena libertad y responsabilidad, inalcanzables si no se le garantiza un espacio ajeno a cualquier intromisión.

([1]) Sobre la necesidad de asegurar la dignidad ontológica de todo ser humano véase A. Aparisi, *En torno al principio de dignidad humana*, en *Cuadernos de Bioética*, 54/2004, 257-282.

Antes de que se generalizaran las innovaciones tecnológicas resultaba más sencillo asegurar ese espacio privado mediante ciertos derechos que nos permitían alejar a los demás de lo que considerábamos como algo reservado para nosotros y para los más allegados con quienes quisiéramos compartirlo. Así se reconocieron, junto a una serie de libertades concretas, los derechos a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones como derechos autónomos, pero con estrecha relación entre sí. La capacidad de acumular y procesar datos de los ciudadanos con los nuevos medios tecnológicos provocó en éstos la sensación de una nueva forma de atentar contra ese espacio privado y reservado; los tribunales, a falta de reconocimiento legal explícito, terminarían por darles la razón con el reconocimiento del derecho al control de los datos personales, libertad informática o autodeterminación informativa ([2]).

Las medidas adoptadas tras los atentados de Nueva York, Madrid y Londres aumentaron desconfianza entre los ciudadanos. A las posibles violaciones de la vida privada por parte de empresas y particulares se unió el interés de las fuerzas de seguridad por evitar nuevas acciones terroristas, lo que llevó a no pocos Estados a la aprobación de cuestionables normas de seguimiento de las comunicaciones y de tratamiento de datos personales sin un control judicial efectivo. Todo ello ha supuesto una ingente labor para los tribunales: no resulta sencillo conciliar seguridad y vida privada y dejar a todos contentos.

1. *Hacia el reconocimiento constitucional de la vida privada*

La vía para llegar al reconocimiento de un derecho fundamental – o constitucional – no es única. Cada Estado, según su tradición jurídica – y política –, suele garantizar la dignidad de sus ciudadanos a través de unos derechos que considera imprescindibles para hacerla realidad. Pero unos Estados son más formalistas y otros menos, unos exigen su formulación expresa en el texto constitucional y otros tan sólo requieren que encuentren un fundamento

---

([2]) Sobre los cambios supuestos por la Sociedad de la Información véase en J.J. MEGÍAS QUIRÓS, *Sociedad de la Información: Derecho, Libertad, Comunidad*, Cizur Menor 2007, los capítulos de E.V. DE MORA QUIRÓS, *De la comunidad heroica a la comunidad virtual*, 23-42, M.J. RODRÍGUEZ PUERTO, *Libertad y Derecho en Internet. El mito del ciber-espacio*, 43-93 y Mª.C. DÍAZ DE TERÁN, *El desarrollo de la Sociedad de la Información: pilares para su regulación*, 95-120.

en él. No podemos detenernos a examinar cada una de las modalidades seguidas en la actualidad porque excede de nuestro objetivo, pero sí haremos referencia a las dos vertientes predominantes en cuanto a los derechos relacionados con la vida privada.

La primera de ella sería, a mi juicio, la menos formalista o de mayor libertad jurisprudencial. Aunque con notorias diferencias, entrarían en este grupo las vías seguidas por EE.UU. y Alemania. La segunda, más formalista, concede a la jurisprudencia un papel menos autónomo respecto del texto constitucional, como ocurre en Italia y España; el texto constitucional español, al ser más reciente, pudo recoger – gracias a las doctrinas desarrolladas en la década de los años 70 – bases más explícitas para el reconocimiento de algún derecho más que el italiano, sin necesidad de acudir a una construcción jurisprudencial excesivamente elaborada, pero ni uno ni otro deja las manos libres a los altos tribunales para reconocer nuevos derechos si previamente no se incluye en el texto o si no se le encuentra asiento en los ya existentes ([3]).

La dificultad es menor cuando existe una tradición o textos supranacionales en los que ya han sido recogidos los derechos que por su trascendencia merecen una protección constitucional. Así ocurrió, por ejemplo, con la intimidad, el secreto de las comunicaciones o la inviolabilidad del domicilio. El artículo 12 de la *Declaración Universal de Derechos Humanos* ayudó en este sentido al establecer que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" ([4]). Pero la *Declaración* era tan sólo eso, una declaración, por lo que se hacía preciso establecer

([3]) Se inclinan por analizar y desarrollar lo que literalmente se recoge en los textos constitucionales para proteger y garantizar la dignidad del ser humano y los derechos que le son inherentes. Pero exigen su modificación expresa cuando se quiere dar cabida a nuevos derechos fundamentales derivados de los cambios sociales. La dificultad radica en que en estos campos se suele mezclar lo estrictamente jurídico con lo político, hecho que impide una rápida modificación de las constituciones o de las leyes que la desarrollan para adecuarlas a las exigencias de justicia derivadas de esos cambios, dejando indefensos a los ciudadanos ante claras vulneraciones de su dignidad. Ocurre en España, por ejemplo, con la objeción de conciencia, que al no estar desarrollada por el legislador se convierte prácticamente en un "*flatus vocis*".

([4]) También de 1948, aunque un poco anterior, la *Declaración Americana de los Derechos y Deberes del Hombre*, en su artículo 5, establecía que "toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

mecanismos de garantía que pudieran proteger de verdad y con eficacia tanto la intimidad como el resto de derechos que no podían ser negados a ser humano alguno; para cumplir tal misión se aprobó en 1966 el *Pacto Internacional de Derechos Civiles y Políticos*, cuyo artículo 17 establecía que nadie sería "objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación"; este instrumento contemplaba algunos mecanismos – insuficientes a todas luces – para la salvaguarda de los derechos o reparación por la vulneración de los mismos. Una diferencia considerable entre uno y otro artículo radica en que el segundo texto abría las puertas a las injerencias "legales", es decir, resaltaba que la vida privada no queda bajo el dominio absoluto de cada individuo y que es susceptible de límites legales por el bien de la sociedad.

Ni uno ni otro texto hacían referencia alguna a la protección de datos porque por entonces no había surgido tal necesidad, como tampoco lo había hecho el *Convenio Europeo para la Protección de los Derechos Humanos* al establecer en su artículo 8 que "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia", solamente susceptible de limitación por razones de seguridad, bienestar económico, defensa del orden, prevención de infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás. Habría que esperar hasta 1981, en que se formalizó el Convenio núm. 108, del Consejo, *para la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal* ([5]), para contar con un texto internacional importante sobre esta materia, pero algunos Estados ya se habían planteado introducir en sus ordenamientos internos determinadas garantías. Más tarde se añadirían referencias, por ejemplo, en la *Declaración del Parlamento Europeo sobre Derechos y Libertades Fundamentales* de 1989, en la *Convención de los Derechos del Niño* de 1990 y en la *Carta Europea de Derechos Fundamentales*, aprobada en Niza en diciembre de 2000, que reconoce de forma separada el derecho al respeto de la vida privada y familiar, de su domicilio y del secreto de sus comunicaciones (artículo 7) y el derecho a la protección de los datos de carácter personal (artículo 8), que había encontrado acomodo en los ordena-

([5]) Modificado en junio de 1999, fue uno de los textos internacionales más importantes. España se cuenta entre los primeros Estados que lo ratificaron, junto con Alemania, Noruega, Suecia y Francia.

mientos internos – por su relación con la intimidad – por diversas vías ([6]).

El reconocimiento de los derechos relacionados con la vida privada en Alemania entronca directamente con la necesidad de asegurar el desarrollo personal de cada ciudadano, imprescindible para que el respeto de su dignidad sea real. Su Ley Fundamental no contempla de modo expreso el derecho a la intimidad o al dominio sobre los datos personales, pero cuenta con una fórmula amplia y abierta en su artículo 2.1 que permite el reconocimiento de éstos y cuantos derechos sean precisos para asegurar el libre desarrollo de la personalidad, siempre que no se lesionen los derechos de los demás y no se contravenga el orden constitucional y las buenas costumbres ([7]). Ello permitió que la jurisprudencia constitucional reconociera en un primer momento la necesidad de asegurar el derecho a la intimidad de las personas como algo imprescindible para asegurar su desarrollo sin injerencias o coacciones externas, estableciendo tres grados distintos de protección según la sensibilidad de la información afectada. Se trataba de un derecho que permitía impedir a los demás el conocimiento de lo más o menos íntimo de un modo compatible con la libertad de información. Pero los avances tecnológicos introdujeron un nuevo peligro al facilitar el tratamiento de datos personales que, aisladamente y por ser públicos o no íntimos, aparentemente no entrañaba riesgo alguno para el desarrollo personal. La práctica demostró que el tratamiento de esos datos permitía elaborar un perfil íntimo de los titulares y, por tanto se vio necesario, reconocer el derecho de control sobre tales datos. No bastaba, por tanto, con una simple facultad de excluir a los demás del conocimiento de lo íntimo, sino que se vio necesario reconocer un dominio sobre los datos públicos que pudieran permitir el acceso a la intimidad, y así fue como el Tribunal Constitucional – al juzgar la Ley del Censo de 1982 – reconoció el derecho a la autodeterminación informativa o *Informationelle Selbstimmungrecht* con todos sus contornos sin necesidad de proceder a la modificación de la Ley Fundamental ([8]). Es digno de elogio este modo de proceder por su efecti-

---

([6]) Sobre la tutela jurídica de la vida privada en el ámbito europeo, véase R. Martínez Martínez, *Una aproximación crítica a la autodeterminación informativa*, Madrid 2004, 211-233.

([7]) Cfr. M.M. Serrano Pérez, *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid 2003, 60-62.

([8]) Cfr. R. Martínez Martínez, *op. cit.*, 237-244.

vidad en la introducción de nuevas garantías jurídicas a causa de exigencias de justicia que surgen en el seno de la sociedad con el paso del tiempo o por el cambio de las circunstancias, pues presta mayor atención a la efectiva protección de la dignidad que a los formalismos propios del positivismo jurídico contemporáneo.

En este sentido puede ser destacado también el camino seguido por EE.UU. hasta el reconocimiento constitucional de la *privacy* como garantía de la dignidad ([9]). Fue en una sentencia de 1873 cuando un tribunal norteamericano utilizó por primera vez el término *privacy* con una pretensión jurídica. En ella se apoyaron años más tarde los abogados Warren y Brandeis para escribir su artículo *The Right to Privacy* ([10]), en el que defendieron la existencia de un derecho a preservar la "privacidad" de posibles injerencias no consentidas por parte de terceros. Aunque la reivindicación tenía su fundamento, los tribunales pusieron objeciones para reconocer una protección jurídica del entorno personal, inexistente hasta el momento. Tras una serie de sentencias titubeantes y contradictorias, la dictada en 1905 por la Corte Suprema de Georgia en el caso *Pavesick vs. New England Life Insurance Company* sería decisiva, pues reconocería que la persona contaba con unos derechos, entendidos como derechos naturales, que debían ser respetados tanto por las autoridades legítimas como por los particulares. Entre estos derechos se encontraba el de la "libertad personal", en su doble vertiente de derecho a la vida pública y del derecho correlativo a la intimidad ([11]).

Años más tarde, siendo Brandeis magistrado de la Corte Suprema de EE.UU., se consagró al amparo de la Cuarta Enmienda de forma definitiva el reconocimiento de ese nuevo ámbito personal merecedor de protección jurídica. La citada Enmienda – referida a

---

([9]) R. Martínez Martínez ofrece un estudio detenido y profundo sobre la *privacy* norteamericana – en sus perspectivas doctrinal, legislativa y jurisprudencial – en *op. cit.*, 66-151.

([10]) Ch. Warren y L., D. Brandeis, *The Right to* Privacy, en *Harvard Law Review* 4/1890, 193-200. El origen de este artículo estuvo en el acoso al que fue sometida – por parte de la prensa – la familia Warren, objeto de críticas continuas por su forma de vida. Warren, con buena formación jurídica, acudió a su amigo – y también abogado – Brandeis con la propuesta de iniciar un trabajo que justificara la necesidad de proteger jurídicamente aquello que veía atacado en su familia sin causa legítima y limitar así la intrusión de la prensa en determinadas esferas que debían tener la consideración de privadas.

([11]) Cfr. L. Rebollo, *El derecho fundamental a la intimidad*, Madrid 2000, 62-63.

la propiedad privada – trata de proteger el derecho de los ciudadanos a la seguridad en sus personas, casas, documentos y efectos de registros, arrestos y embargos sin causa suficiente, pero también contempla la ilicitud de cualquier orden de registro o arresto que no contenga una motivación fundada, así como la descripción del lugar que deba ser registrado o de las personas o cosas sobre las que recaiga la orden. A partir de los años 30 comenzó a servir de fundamento para proteger la intimidad, pero fue en 1965 cuando esta protección adquirió el rango de derecho constitucional con un contenido identificado con la "autonomía para tomar decisiones íntimas" ([12]), y con la característica más propia de los derechos humanos de la primera generación: la exclusión de terceros de ámbitos que se entienden reservados al titular del derecho ([13]).

Dado que en Estados Unidos se aprecia aún la preeminencia del derecho de propiedad, no sólo sobre las cosas materiales, sino también sobre todo lo que concierne a la persona, no resulta difícil comprender que el ámbito de la *privacy* fuera concebido en un principio como una esfera en la que sólo cada persona podía decidir si permitía o no a los demás participar de su conocimiento, de modo que la facultad principal consistía en algo negativo – excluir –, no en llevar a cabo acciones concretas o en controlar determinados datos. En la mentalidad continental europea, por el contrario, fue más sencillo sostener desde un principio una concepción de estos derechos sin quedar reducidos a facultades negativas o de exclusión, prestando también atención a su vertiente positiva o de control de datos. No obstante, el legislador y la jurisprudencia norteamericana pudieron introducir en la década de los años 70 con bastante flexibilidad las garantías de control por parte de los titulares que se estimaron precisas, alcanzando una notable influencia en el ámbito anglosajón ([14]).

En España e Italia el formalismo es mayor y los tribunales constitucionales gozan de una maniobrabilidad más limitada a la hora de configurar nuevos derechos, de ahí las numerosas discusio-

---

([12]) Cfr. B. Rodríguez Ruiz, *El secreto de las comunicaciones: tecnología e intimidad*, Madrid 1998, 4-6 y 20-21.

([13]) Véase, sobre las características de estos derechos, J. Ballesteros *Postmodernidad: decadencia o resistencia*, Madrid 1989, 56 ss.

([14]) Para un estudio más completo en el ámbito anglosajón véase M. Tugendhat, I. Christie, *The law of privacy and the media*, Oxford 2002; P. Carey, *E-privacy and online data protection*, London 2002; Id., *Data protection: a practical guide to U.K. and EU law*, Oxford 2004.

nes doctrinales – durante las tres últimas décadas – hasta dejar bien perfilados los derechos que preservan la vida privada. En uno y otro país han tenido gran resonancia las construcciones de la *privacy* norteamericana y de la autodeterminación informativa – o libertad informática – alemana, pero los efectos jurídicos derivados de estas dos figuras han debido ser justificados por otras vías. La amplitud de la *privacy* hizo que se descartara su equiparación con los derechos a la "intimidad" o "*riservatezza*", salvo que se modificara el significado de éstas para convertirlas en algo más amplio. El sector doctrinal mayoritario descarta la posibilidad de hablar de un derecho a la vida privada, pero admiten esta expresión como un concepto amplio que acoge una multiplicidad de derechos autónomos interconexionados entre sí.

De forma muy resumida, podríamos decir que en Italia la doctrina centra el fundamento de estos derechos en los artículos 2, 13, 14, 15 y 21 de la Constitución ([15]). El primero alude a la necesidad de reconocer unos derechos inviolables que aseguren el libre desarrollo personal, derechos que deben encontrar asiento a su vez en otros preceptos constitucionales, y aquí es donde entran en juego los otros artículos citados, referidos a la libertad, la inviolabilidad del domicilio, el secreto de las comunicaciones y la libre manifestación del pensamiento y de información como presupuestos indispensables de un libre desarrollo personal. No obstante, no se trata de una lista cerrada; existen otros presupuestos necesarios para el libre desarrollo personal que sólo serían reconducibles al artículo 2, como ha venido a reconocer la Corte Constitucional italiana en diversas ocasiones, lo que le otorga al citado artículo un cierto carácter de cláusula abierta siempre que se pueda poner en conexión tal presupuesto con algún derecho expresamente reconocido en el texto constitucional, lo que lo diferencia del artículo 2.1 alemán ([16]). A este

---

([15]) La amplia obra de Vittorio Frosini ofrece una visión completa de la evolución doctrinal en torno a la vida privada en la Sociedad de la Información. Entre la bibliografía más reciente pueden consultarse A. LOIODICE, G. SANTANIELLO, *La tutela Della riservatezza*. Padova 2000; G. ARNÒ, *La tutela Della privacy nella rete Internet*. Torino 2002; A. SCALISI, *Il diritto alla riservatezza*, Milano 2002; A. LISI, *La privacy in Internet*, Napoli 2003; *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, a cura di R. Acciai, Rimini 2004; G.P. CIRILLO, *Il codice sulla protezione dei dati personali*, Milano 2004; G. ELLI, R. ZALLONE, *Il nuovo codice della privacy*, Torino 2004; G. SATOR, J. MONDUCCI, *Il Codice in materia di protezione dei dati personali*, Padova 2004.

([16]) Cfr. Mª.M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos*, cit., 41-49.

carácter de cláusula abierta es al que hay que recurrir para fundamentar la libertad informática como derecho constitucional. Así lo puso de manifiesto reiteradamente V. Frosini – y con él otros muchos autores –, poniéndola en conexión con el artículo 13 al entender que se trataba de una nueva modalidad de libertad personal, física y moral, en una sociedad afectada y transformada por las innovaciones tecnológicas posteriores al texto constitucional. Se encuadraría en esta nueva libertad personal tanto la facultad de no entregar la información sensible que pudiera condicionar el libre desarrollo personal, como la facultad de controlar los datos personales y el uso que se hiciera de ellos por parte de quienes los hubieran conseguido con nuestro consentimiento o con autorización legal.

En el caso de España el reconocimiento de estos derechos ha sido más sencillo por contar con un texto constitucional más reciente que se ha servido de los avances legislativo y jurisprudencial de otros países. Reconoce de forma expresa en el artículo 18 el derecho a la intimidad (párrafo 1º), a la inviolabilidad del domicilio (párrafo 2º), al secreto de las comunicaciones (párrafo 3º), así como una fórmula amplia (párrafo 4º) que limita el uso de los medios informáticos cuando de ello pudiera derivarse algún riesgo de lesión de la intimidad, fórmula de la que se sirvió el Tribunal Constitucional en 1993 para dar cabida a la libertad informática o autodeterminación informativa como derecho fundamental autónomo ([17]). Se descarta, por tanto, la posible confusión entre intimidad y vida privada (la *privacy* norteamericana). La primera tiene como objeto propiamente excluir a los extraños del conocimiento de nuestros datos íntimos, mientras que la segunda conlleva no sólo el respeto de éstos, sino también su control, así como el secreto de las comunicaciones y de las circunstancias en que se producen, el control de otros datos públicos que dan acceso a la intimidad ([18]), etc. Por su naturaleza, podríamos afirmar que el secreto de las comunicaciones, o la inviolabilidad del domicilio, o incluso en ocasiones el control de datos, son

([17]) Sobre la configuración constitucional de estos derechos en el ordenamiento español véase R. Martínez Martínez, *op. cit.*, 245-314 y 323-343.

([18]) La Exposición de Motivos de la Ley Orgánica 15/1999, de 13 de diciembre, de *Protección de Datos de Carácter Personal* (LOPD) se hizo eco de esta diferencia al manifestar que "la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".

derechos que están al servicio de la intimidad, pues lo que se pretende con ellos es evitar que se llegue al conocimiento de ésta. El derecho a la intimidad, como núcleo esencial de la vida privada, tendría, por tanto, un carácter material, mientras que los otros derechos tendrían un carácter más formal; es decir, para evitar el conocimiento de la intimidad, toda comunicación debe ser secreta, o todo domicilio debe ser inviolable, o todos los datos personales deben permanecer bajo el control de su titular ([19]), salvo que haya una causa justificada para permitir lo contrario. El simple hecho de intervenir una comunicación no implica forzosamente que podamos llegar a lo íntimo – dependerá de su contenido –, pero lo que no se puede negar es que constituye un medio idóneo para conseguirlo ([20]).

Como consecuencia de estas distinciones, también se reivindica una protección diferente, acorde a cada ámbito. La intimidad, donde se sitúa "el ámbito de los pensamientos de cada cual, de la formación de las decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado y que quizás nunca lo será…", debe estar protegida por un "velo de total opacidad que sólo podría ser levantado por el individuo mismo" ([21]). En cambio, la "privacidad" sería un ámbito donde imperan exclusivamente los deseos y preferencias individuales, condición necesaria del ejercicio de la libertad individual, y que podría denominarse "esfera personal reconocida"; sus límites dependerían del contexto cultural y social, de modo que el velo que la cubre debería ser de una transparencia relativa.

([19]) Ya en 1984 dejaba claro el Tribunal Constitucional que era necesario proteger determinados ámbitos para proteger la intimidad, manifestando que los avances tecnológicos obligaban "a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida" (STC 110/1984, Fundamento Jurídico 3º).

([20]) Así lo ha vuelto a declarar la STC 70/2002, en el Fundamento Jurídico 9º al estimar que "El concepto de lo secreto tiene carácter formal: 'El concepto de secreto en el artículo 18.3 tiene un carácter formal, en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado'".

([21]) E. Garzón Valdés, *Privacidad y publicidad*, en *Doxa* 21-1/1998, 226.

1.1. El derecho a la intimidad

Al establecer Yepes Stork las notas que definen a la persona, afirmaba que la primera de ellas es la intimidad, como grado máximo de la inmanencia o *apertura hacia dentro* que corresponde a cualquier ser humano ([22]). Es la nota que nos permite a cada uno ser nosotros mismos y de ahí su importancia y necesidad de protección, pues en ella entronca el rumbo que le demos a nuestras actuaciones y, en definitiva, a nuestra vida. No se trata solamente de proteger algo interno de las miradas extrañas, sino de permitir que ese algo "interno" guíe sin intromisiones ilegítimas el pleno desarrollo de cada persona de acuerdo con su dignidad. "La característica más importante de la intimidad es que no es estática, sino algo vivo, fuente de cosas nuevas, creadora: siempre está como en ebullición, es un núcleo del que brota el mundo interior. Por ahí se puede ver que ninguna intimidad es igual a otra, porque cada una es algo irrepetible, incomunicable: nadie puede ser el yo que yo soy. La persona es única e irrepetible, porque es un *alguien*; no es sólo un *qué*, sino un *quién*. La persona es la contestación a la pregunta ¿quién eres? Persona significa inmediatamente quién, y quién significa un ser que tiene nombre, que es alguien ante los demás" ([23]). Si arrebatáramos la intimidad a una persona, estaríamos atacando directamente su dignidad, lo más vulnerable del ser.

Aunque la persona vive en sociedad, rodeado de otras muchas personas ante las que debe dar cuenta de innumerables actuaciones, sin embargo tiene también la necesidad de volverse hacia su interior y meterse dentro de sí. No solemos adoptar nuestras decisiones de un modo irreflexivo, instintivamente, sino que éstas suelen ser el resultado de un proceso racional interno en el

---

([22]) "La intimidad es el grado máximo de la inmanencia, porque no es sólo un lugar donde las cosas quedan guardadas para uno mismo sin que nadie las vea, sino que además es, por así decir, un dentro que crece, del cual brotan realidades inéditas, que no estaban antes: son las cosas que se nos ocurren, planes que ponemos en práctica, invenciones, etc. La intimidad tiene capacidad creativa. Por eso la persona es una intimidad de la que brotan novedades, una intimidad creativa, capaz de crecer" y que cuando se muestra al exterior supone una "manifestación de la intimidad" (R. Yepes Stork, *Fundamentos de Antropología*, Pamplona 1996, 76-77).

([23]) Ivi, 78. Afirma un poco antes que "lo íntimo es tan central al hombre que hay un sentimiento natural que lo protege: la vergüenza o pudor, que es, por así decir, la protección natural de la intimidad, el cubrir u ocultar espontáneamente lo íntimo frente a las miradas extrañas". Cfr. también R. Spaemann, *Personas. Acerca de la distinción entre "algo" y "alguien"*, Pamplona 2000.

que han intervenido sentimientos, forma de pensar, deseos, anhelos, (…) que normalmente no deseamos revelar a los demás. Es más, en numerosas ocasiones nos comportaríamos de modo distinto si no pudiéramos mantener "retirado" de los demás ese proceso de toma de decisiones. Esta necesidad de la persona de retirarse a un lugar interior discreto es precisamente lo que viene a proteger el derecho a la intimidad y, en definitiva, lo que nos permite desarrollar la personalidad propia que quedará reflejada en nuestro comportamiento externo, porque la intimidad no se agota en la interioridad humana, sino que también condiciona la acción. La soberanía del ser humano sobre sus acciones no puede consistir simplemente en no encontrar impedimentos para ejecutarlas, sino que excluye también la mirada ajena durante la decisión, puesto que esa mirada ajena puede condicionarnos en el modo de comportamiento. Como afirma L. García San Miguel, la intimidad sería "el derecho a no ser conocidos, en ciertos aspectos, por los demás. Es un derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos" ([24]). E. Garzón llega a dar por válido que el paso desde lo privado hacia lo público pueda estar caracterizado, incluso, por la hipocresía y la reducción de la verdad, de modo que cuando no nos sea posible evitar la curiosidad ajena y "malsana" de nuestra intimidad podría ser lícito actuar de acuerdo con lo "políticamente correcto", aunque no responda exactamente a la verdad de lo que sentimos y pensamos ([25]).

Este derecho a la intimidad lo definiría el Tribunal Constitucional español como "un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario – según las pautas de nuestra cultura – para mantener una calidad mínima de la vida humana" ([26]). Esta fórmula, más o menos general, permite incluir en

---

([24]) L. García San Miguel, *El derecho a la intimidad*, en Aa.Vv., *Diccionario crítico de derechos humanos*, Huelva 2000, 258.

([25]) Cfr. E. Garzón Valdés, *Privacidad y publicidad*, cit., 231. Previamente ha sentado la base de que la revelación de lo íntimo es discrecional por parte de su titular, y "ello explica por qué la revelación voluntaria de nuestra intimidad solemos hacerla sólo en caso de relaciones excepcionales como las que crea el amor o un cierto tipo de amistad que justamente llamamos 'íntima'. En estos casos la revelación suele ser recíproca y es considerada como forma más auténtica de entrega al otro. Está también, desde luego, la transmisión de secretos al confesor, o su versión laica, el psicoanalista" (229).

([26]) STC 231/1988, Fundamento Jurídico 3º; esta idea ha sido reiterada en las SSTC 179/1991, Fundamento Jurídico 3º, 20/1992, Fundamento Jurídico 3º, 57/1994, Fundamento Jurídico 5º, 143/1994, Fundamento Jurídico 6º, etc.

ese ámbito no sólo los datos, sucesos, acciones, etc., que se produzcan en la intimidad, sino también todo aquello que, aún siendo público y notorio, o bien ha sido difundido más allá del ámbito en que tenía sentido su conocimiento, o bien puede dar acceso a la intimidad al ponerlo en conexión con otros datos ([27]). Este segundo supuesto se enmarcaría concretamente en lo que se ha denominado "teoría mosaico": un dato conocido públicamente, pero aislado, puede ser inocuo, pero puesto en conexión con otros datos también públicos puede revelar el perfil íntimo de una persona. Las Nuevas Tecnologías permiten la obtención de estos datos, su almacenamiento, su tratamiento, etc., hasta indicarnos, por ejemplo, si conviene a un empresario contratar a un determinado trabajador o si a una aseguradora le compensa mantener a determinados asegurados, etc.

Por ello distingue el Derecho entre la facultad de excluir los datos del conocimiento ajeno y la de controlarlos. En el primer caso nos encontraríamos ante el derecho a la intimidad, cuya función es proteger frente a cualquier invasión que pueda realizarse "en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad" ([28]). El segundo, por el que podemos proteger nuestros datos, nos garantiza – como veremos más adelante – "un poder de control sobre los datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado" ([29]).

Esta importancia de la intimidad es la que hace necesaria adoptar las medidas precisas frente a las injerencias que puedan derivar de la utilización de las Nuevas Tecnologías en la Sociedad de la Información, en particular en todo lo referido al secreto de las comunicaciones y al control de datos personales.

([27]) Es difícil obtener una definición de dato íntimo que salve todas las dificultades. Podríamos definirlo como aquél que se produce en la intimidad y que carece de trascendencia para la vida social, de modo que ésta podría continuar su curso sin resentirse a pesar de su ignorancia. Pero esta definición nos sirve a medias solamente, pues con ella tendríamos que valorar en cada caso si algo íntimo repercute o no. Por ejemplo, puede pertenecer a la intimidad el hecho de que una persona sea heroinómana, y que no podamos ir preguntándole a los demás si son drogadictos. Pero ¿qué pasaría si esa persona es anestesista y puede contagiar una enfermedad como la hepatitis a los pacientes que llegan al quirófano? Pues que entrar a conocer ese dato no supondría una violación de la intimidad, ni tampoco lo sería informar sobre ello si se hubieran producido los contagios.

([28]) STC 144/1999, de 22 de julio, Fundamento Jurídico 8º.

([29]) STC 292/2000, de 30 de noviembre, Fundamento Jurídico 6º.

1.2. El derecho al secreto de las comunicaciones

Tuvo un reconocimiento en los textos constitucionales muy anterior al derecho a la intimidad. En España fue reconocido por primera vez en los arts. 7 y 8 de la Constitución de 1869, y posteriormente en las de 1876 (artículo 7) y 1931 (artículo 32). Actualmente el artículo 18.3 establece que "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial". Aunque tan sólo recoge las más comunes, la expresión "en especial" supone que pueda quedar protegida cualquier tipo de comunicación realizada a distancia, por lo que no se puede albergar dudas sobre si la comunicación electrónica queda amparada o no. La Sentencia del Tribunal Constitucional 70/2002, de 3 de abril, tuvo que realizar una llamada de atención al legislador español al afirmar en su noveno Fundamento Jurídico que "Ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del artículo 18.3". No entró en más profundidades, pero al menos dio a entender que no era ajeno a los avances en este terreno.

El derecho al secreto de las comunicaciones se caracteriza por ser al mismo tiempo un derecho *autónomo* del derecho a la intimidad e *inseparable* de ésta ([30]), pues no se pretende salvaguardar solamente el secreto de todo cuanto concierne a las comunicaciones privadas – aquí radica la autonomía –, sino también el acceso a lo íntimo a través de la interceptación. A diferencia de la intimidad, ha sido entendido de forma mayoritaria como un derecho de carácter formal, es decir, que siempre que se produce una injerencia sin la correspondiente autorización judicial, se consuma un atentado contra este derecho. Sin embargo, el Tribunal Constitucional español no lo ha entendido así, pues su modo de enjuiciar las demandas de amparo consiste en constatar primero si se ha producido una inje-

([30]) Esta idea es repetida constantemente a lo largo de la obra de B. RODRÍGUEZ, *op. cit.*, 1, 4, 14, 20-21, 24, ss. Considera que la intimidad constituye un derecho más flexible en cuanto a su contenido (puede proteger también las conversaciones y comunicaciones privadas), por ello, cuando alguna de sus zonas de protección pueden ser bien definidas, como ocurre con las comunicaciones, "dichas zonas deben ser reconocidas como derechos independientes" (4).

rencia y, en caso afirmativo, valorar si tiene algún tipo de justificación, aunque se haya producido sin la preceptiva resolución judicial ([31]); combina, pues, el carácter formal y el material para realizar un juicio de valor ([32]). Con ello se sitúa en una posición intermedia entre la mantenida por el Tribunal Constitucional alemán, más abierto a las limitaciones del derecho, y la que defiende el Tribunal Europeo de Derechos Humanos, que admite como única justificación de la injerencia el cumplimiento de todos los requisitos establecidos legalmente para llevarla a cabo ([33]). La suspensión del derecho está contemplada por el artículo 55 de la Constitución española para los casos de estado de excepción o sitio y en la persecución de las actividades de bandas armadas y terroristas, en cuyo caso podría hablarse más de una restricción especial que de una suspensión, pues el texto constitucional es más permisivo en este caso si se rebasaran los límites legales. La razón de esta mayor permisibilidad es que se pretende evitar un daño a la sociedad – mediante el ataque de sus valores y principios constitucionales – causado por uno o

([31]) Así, podemos leer en la STC 70/2002, de 3 de abril, Fundamento Jurídico 9º que "Esta doctrina – establecida ciertamente en otro ámbito diferente, pero conexo – resulta aplicable también a los supuestos que nos ocupan. La regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad"; y más adelante: "La valoración de la urgencia y necesidad de la intervención policial ha de realizarse *ex ante*, y es susceptible de control judicial *ex post*, al igual que el respeto del principio de proporcionalidad. La constatación *ex post* de la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales".

([32]) En sentido contrario a este modo de proceder se pronuncia J. Jiménez Campos, que entiende que la intimidad tiene siempre un contenido material, mientras que el secreto de las comunicaciones es rigurosamente formal, pues "toda comunicación es, para la norma fundamental, secreta, aunque sólo algunas, como es obvio, serán íntimas" (*La garantía constitucional del secreto de las comunicaciones*, en *Revista Española de Derecho Constitucional*, 20/1987, 41).

([33]) Cfr. B. Rodríguez, *op. cit.*, 55-62.

varios ciudadanos con el ejercicio abusivo de un derecho fundamental, como es el secreto de las comunicaciones en este caso.

Por otro lado, es preciso resaltar que el secreto de las comunicaciones no afecta solamente al contenido de las mismas, sino a determinados datos relacionados con las comunicaciones que nos podrían revelar información relevante de la vida privada de los comunicantes. Así lo ha reiterado el Tribunal Europeo de Derechos Humanos y también el Tribunal Constitucional español ([34]). Entre estos datos protegidos cabe destacar la dirección electrónica, la dirección IP, etc.

1.3. La libertad informática o autodeterminación informativa

Este derecho tuvo su primer reconocimiento constitucional europeo en Alemania. España tuvo que esperar hasta la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio ([35]). Las SSTC 290/2000 y 292/2000, de 30 de noviembre, supusieron un paso definitivo en su consolidación detallada, y se ha establecido un marco más acorde a los nuevos avances tecnológicos con la aprobación de la Ley 34/2002, de 11 de julio, *de servicios de la Sociedad de la Información y de Comercio Electrónico* y la Ley 56/2007, de 28 de diciembre, de *Medidas de Impulso de la Sociedad de la Información*. Aunque la generalidad de la doctrina, incluido el Tribunal Constitucional, fundamenta este derecho – también llamado derecho de libertad informática – en el artículo 18.4, no falta quien prefiere recurrir a otra fundamentación del mismo, como ocurre con M.

([34]) Baste citar la Sentencia del Tribunal Constitucional 230/2007, 5 de noviembre, que recoge la doctrina reiterada en otras anteriores. En su Fundamento Jurídico segundo afirma que "Igualmente se ha destacado que el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores, de ahí que se haya afirmado que la entrega de los listados de llamadas telefónicas por las compañías telefónicas a la policía, sin consentimiento del titular del teléfono, requiere resolución judicial, toda vez que el acceso y registro de los datos que figuran en dichos listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones".

([35]) Cuya doctrina ha sido reiterada con posterioridad, entre otras, en las SSTC 143/1994, 9 de mayo (que se pronunciaba sobre el uso del NIF), 11/1998, 13 de enero, y 94/1998, 4 de mayo (ambas sobre datos de afiliación sindical), 202/1999, de 8 de noviembre (sobre datos médicos), etc. Sobre la Sentencia 254/1993, véase L.M. ARROYO, *El derecho a la autodeterminación informativa frente a las Administraciones Públicas*, en *Revista Andaluza de la Administración Pública*, 16/1993, 122 ss.

Jiménez de Parga, que en su voto particular a la Sentencia 290/2000 negaba su contemplación expresa en el texto constitucional y defendía su vertebración a partir del artículo 10.1 en relación con los artículoss 18.1 y 20.1 ([36]).

Fue el Tribunal Constitucional alemán el primero en establecer unas directrices claras al enjuiciar la Ley del Censo alemana de 1982, pues vislumbró que tan importante era reconocer unas esferas personales dignas de protección y reservadas frente al conocimiento ajeno, como reconocer las facultades de control de tales zonas y de los datos que se generaran en ellas. Quedaba configurado así un derecho que otorgaba a cada persona el control sobre la información que pudiera obtener el poder público o las personas privadas y el uso que pudieran hacer de ella ([37]). El Tribunal Constitucional español admitió en 1993 que "la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada *libertad informática* es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos" ([38]). La Sentencia 292/2000 daría por admitida esta doctrina de forma unánime en sus Fundamentos Jurídicos 4º y 5º.

Afortunadamente, el legislador comunitario ha realizado un notable esfuerzo por establecer una legislación de desarrollo de este derecho, aunque el resultado no haya sido todo lo idóneo que se esperaba. La primera Directiva de trascendencia fue la 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al trata-

---

([36]) Afirma que "los cimientos constitucionales para levantar sobre ellos el derecho de libertad informática son más amplios que los que proporciona el artículo 18.4 CE". Voto particular, apartado 4.

([37]) B. Rodríguez, *op. cit*, 14-15. Considera que este derecho es inseparable de la intimidad; sería, efectivamente, como la otra cara de la moneda, distinto, pero inseparable de la faceta negativa o excluyente (cfr. 15-17). Véase una opinión crítica sobre la argumentación del Tribunal Constitucional alemán, por su complejidad, en A.E. Pérez Luño, *Biotecnologías e intimidad*, en *La tercera generación de derechos humanos*, Cizur Menor 2006, 130-132.

([38]) STC 254/1993, de 20 de julio, Fundamento Jurídico 7º. En el Fundamento Jurídico anterior declara que el artículo 18.4 establece un derecho fundamental claro, "el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática', lo que se ha dado en llamar *libertad informática*".

miento de los datos personales y a su libre circulación. La segunda es de julio de 2002 (2002/58/CE), relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que derogó otra de 1997. La última, que modifica en parte la anterior, es la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, relativa a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicación electrónica ([39]). En ella queda reflejada la preocupación del legislador comunitario por el uso indebido que pueda realizarse de datos concernientes al origen y destino de la comunicación, fecha, hora y duración, equipo utilizado y localización de los usuarios ([40]). El Tribunal Europeo de Derechos Humanos ha seguido también unos criterios reiterados en sus sentencias, con una clara relevancia para las legislaciones y jurisprudencias internas de los Estados ([41]).

El objeto de este derecho, como tiene declarado la jurisprudencia en general, es más amplio que el objeto del derecho a la intimidad, pues incluiría también la protección de cuanto fuera preciso para el pleno ejercicio de los derechos de la persona, es decir, aquellos datos relevantes para el ejercicio de cualquier derecho relacionado con el honor, la ideología, la intimidad personal o familiar, o a cualquier otro bien constitucionalmente amparado ([42]). Además, co-

---

([39]) Sobre su posible nulidad véase M.C. Guerrero Picó, *Operadores privados y seguridad pública: la retención de los datos de tráfico a la luz de la sentencia PNR*, en *Revista Española de Protección de Datos* 2/2007, 185-215. En el ordenamiento jurídico español tendríamos que destacar, naturalmente, la LO 15/1999, de 13 de diciembre, de *Protección de Datos de Carácter Personal* y algunos artículos de la Ley 32/2003, de 3 de noviembre, *General de Telecomunicaciones* y la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones* (hoy recurrida ante el Tribunal Constitucional). Entre las normas de rango inferior, muy numerosas, tiene especial relevancia el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

([40]) Cfr. P. Lucas Murillo de la Cueva, *Perspectivas del derecho a la autodeterminación informativa*, en *IDP*, 5/2007, 25-26.

([41]) Véase, por ejemplo, Sentencia de 16 de febrero de 2000, *Asunto Amann c. Suiza*, Sentencia de 4 de mayo de 2000, *Asunto Rotaru c. Rumania*, y, más recientemente, Sentencia de 3 de abril de 2007, *Asunto Copland c. Reino Unido*. Para un visión detenida de la jurisprudencia del Tribunal Europeo sobre la protección de la vida privada, véase R. Martínez Martínez, *op. cit.*, 155-211.

([42]) STC 292/2000, Fundamento Jurídico 6º. En concreto, "los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

mo he advertido anteriormente, podríamos afirmar que su objetivo tiene un cierto carácter formal, pues trata de evitar que un extraño consiga llegar hasta lo que propiamente constituye la intimidad de la persona mediante el tratamiento de datos que han podido ser obtenidos lícitamente ([43]).

Para evitar que pueda resultar afectada la intimidad, las normas coinciden en establecer una serie de principios que deben regir bien en el momento de recoger los datos, bien en el momento de su tratamiento. La recolección de datos personales debe estar presidida por los principios de *justificación legal y social* (motivo lícito para llevarla a cabo), de *licitud y limitación* (a través de medios lícitos – legales y consentidos – y sólo aquellos datos necesarios para cumplir con el fin que se persigue), de *fidelidad a la información* (deben ser datos completos, exactos y actuales, con posibilidad de ser rectificados cuando falte alguna de estas características) y de *pertinencia y finalidad* (sólo se deben conservar para la finalidad perseguida lícitamente).

Entre los principios que deben regir el tratamiento y procesamiento de los datos ya recogidos, encontramos el de *confidencialidad de los datos* (incluye a la entidad y a sus trabajadores), el de *seguridad* (el responsable de los archivos debe disponer las medidas para preservarlos del conocimiento ajeno), el de *caducidad* (deben mantenerse solamente hasta que se alcance el fin perseguido, procediéndose a la cancelación inmediatamente después) y el de *autonomía de la voluntad* (cualquier tratamiento debe ser previamente consentido por el titular de los datos). Aunque todos estos principios han informado las citadas Directivas y las normas internas, en un primer momento se incurrió en el error de proteger a los ciudadanos fundamentalmente frente a los abusos por parte del sector público, pasando de puntillas por el ámbito del sector privado. Las últimas modificaciones de las normas han introducido mecanismos para hacerlos efectivos tanto frente a la administración pública como frente a cualquier particular.

Hemos hecho notar anteriormente que las facultades que nos otorga el derecho de intimidad son negativas, de exclusión de la

([43]) Se aprecia una diferenciación entre simples datos personales (nombre, dirección, etc.) y datos personales sensibles, referidos éstos últimos al origen racial o étnico, ideología, creencias religiosas o filosóficas, afiliación sindical, salud o vida sexual. Los segundos tienen un nivel mayor de protección, necesitándose para su tratamiento un consentimiento explícito del interesado o una causa estricta contemplada en la legislación.

mirada extraña, comprendiendo aquellos datos que siendo públicos rebasan su ámbito de conocimiento propio o aquellos que puestos en relación con otros revelan la intimidad. Lo propio del derecho a la libertad informática es que nos otorga facultades positivas, de acciones concretas, erigiéndonos en señores de la información personal que generamos. Si en la realidad no podemos hacer uso de esas facultades, nuestro derecho será teórico e ineficaz. Estas facultades se podrían resumir en: consentir la recogida – la obtención y el acceso a los datos personales –, consentir su posterior almacenamiento y tratamiento, consentir su uso o usos posibles por un tercero, saber en todo momento quién dispone de esos datos y qué usos hace de ellos, y, por último, la de denegar esa posesión y uso ([44]). Es decir, la libertad informática atribuye un "haz de facultades" por las que el sujeto de derecho puede imponer a terceros la realización u omisión de determinados comportamientos relacionados con el uso de la informática que le afectan a él personalmente.

El Tribunal Constitucional español declaró inconstitucionales determinados incisos de la LOPD por no haber establecido unas garantías precisas y eficaces de estas facultades. Los artículos 21 y 24 había abierto las puertas a cesiones de datos sin previa información (y preceptiva autorización) a través de normas reglamentarias sin rango legal: en el caso del "derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la ley apodere a ésta para que precise en cada caso sus límites". Corresponde al legislador y sólo a él determinar cuándo concurre un bien o un derecho que justifique una restricción, en qué circunstancias cabe la limitación y qué reglas precisas deben seguirse, de modo que el afectado pueda prever las consecuencias. Y ello requiere también desterrar las expresiones "interés público" o "intereses de terceros más dignos de protección" por constituir fórmulas abiertas y ambiguas que pueden suponer una restricción arbitraria del derecho por parte de las administraciones públicas.

([44]) STC 292/2000, Fundamento Jurídico 7º. Lo realmente importante será conseguir un control efectivo sobre los datos personales y la información personal que generamos, no sólo para evitar la consecución de perfiles que puedan interesar desde un punto de vista comercial, sino para evitar cualquier retrato de la intimidad de una persona.

2. *Vulneraciones más generalizadas de la vida privada en la Sociedad de la Información*

Resulta imposible, en un estudio breve, recoger un elenco de todas las acciones, públicas o privadas, que suponen un atentado contra la vida privada derivadas de la generalización de las Nuevas Tecnología, pero sí podemos destacar algunas de las más importantes. A ello se añade que es difícil clasificar los riesgos según el derecho afectado, pues, por lo general suele resultar afectado más de uno de ellos al mismo tiempo, y siempre se encuentra de fondo el riesgo generado para la intimidad como núcleo más importante de la vida privada. Por comenzar con un ejemplo reciente, podríamos citar lo acontecido en mayo de 2008 en Italia con la publicación en Internet de los datos de todas las declaraciones de renta correspondientes al año 2005 ([45]). No puede entenderse como una vulneración de la libertad informativa simplemente, sino también de la intimidad, pues los datos pueden reflejar, por ejemplo, preferencias religiosas o ideológicas de los contribuyentes que hubieran realizado donaciones a entidades de carácter religioso o político.

Entre las vulneraciones más importantes acaecidas en los últimos años por parte de entidades públicas ha destacado la famosa red *Echelon*. Creada por varios Estados para espionaje empresarial, fue confirmada su existencia en marzo de 2001 por la Comisión del Parlamento Europeo creada para su investigación, atribuyéndole un papel fundamental en la interceptación de mensajes electrónicos de carácter comercial. Gerhard Schimd, parlamentario y ponente de la Comisión, recomendó en su exposición a los gobiernos, empresas y ciudadanos la utilización de sistemas de cifrado seguro ([46]).

([45]) La Agencia Tributaria colgó durante unas horas en Internet los datos de las declaraciones correspondientes al año 2005. La Autoridad Garante para la Protección de Datos Personales requirió horas después su retirada por entender que vulneraba la ley de protección de datos personales; al día siguiente prohibió definitivamente su publicación. Fuentes del Gobierno comunicaron que se trataba de favorecer la democracia y la transparencia y que ley le confería competencias para tal publicación. La Autoridad Garante reconoció que la ley efectivamente permitía a la Agencia Tributaria elaborar esas listas, pero no elegir los modos de publicación (sin filtros, ni protección en el acceso). La asociación de consumidores Codacons interpuso una demanda contra el ex-Secretario de Estado de Economía (responsable de la decisión) por la que solicitaba una indemnización de 20.000 millones de euros.

([46]) El Parlamento Europeo aprobó por 367 votos a favor, 159 en contra y 34 abstenciones, el informe definitivo de 120 páginas sobre las actividades de la red de espionaje *Echelon.* Gerhard Schmid – autor del informe – consideró probado que este

En cuanto a los seguimientos de comunicaciones y obtención de datos por parte de las Fuerzas de Seguridad, hay que hacer notar que en ocasiones no se ha respetado el equilibrio que debe existir entre los derechos individuales y los intereses generales, ignorándose la necesidad de obtener y procesar los datos legítimamente (legalidad y justicia), con fines específicos previamente establecidos (legalidad) y asegurando la proporcionalidad entre medios utilizados (lo que podemos perder en el camino) y los objetivos que pretendemos alcanzar. Los agentes públicos ocultan en ocasiones que para perseguir a "posibles terroristas" procesan datos (viajes, telecomunicaciones, finanzas, etc.) que afectan a muchas personas inocentes. Ni la erradicación del terrorismo, ni la seguridad del Estado, ni la persecución de la pedofilia, etc., justificarían la interceptación indiscriminada por parte de los poderes públicos. Debe existir una razón y una resolución judicial motivada o, en caso de urgencia, la autorización de una instancia gubernativa prevista en la ley y que pueda responder después de la decisión tomada ([47]).

La psicosis social desencadenada tras los actos terroristas de Nueva York sirvió de justificación para aprobar ciertas normas y actuaciones cuestionables. Pocas horas después de los atentados de 2001, el FBI solicitó a los proveedores de acceso a Internet, servicios web y mensajería electrónica que instalasen el sistema de seguimiento *Carnivore* – DCS1000 –, idóneo para intervenir las comunicaciones realizadas a través de las redes de los ISPs. Podía solicitarlo porque la *Foreing Intelligence Surveillance Act* limitaba la facultad de intervención de comunicaciones, pero no en el supuesto de acciones criminales ([48]). Días más tarde, el Senado aprobaba el proyecto de la *Anti-Terrorism Act*, que concedía al Gobierno un margen mayor en la utilización de la tecnología de vigilancia (intervención

---

sistema de interceptación electrónica de las comunicaciones privadas y de carácter económico contaba con la cooperación de Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda.

([47]) El *Informe Cappato* – aprobado en julio de 2001 por 22 votos a favor, 12 en contra y 5 abstenciones por el Comité de Libertades Civiles del Parlamento Europeo – proponía restricciones a las autoridades policiales comunitarias para interceptar el tráfico de las comunicaciones y su localización, y desestimaba la propuesta de guardar los datos del tráfico de las comunicaciones electrónicas durante siete años.

([48]) Ello permitió a America Online y EarthLink la colaboración con el FBI en la consecución de información privada para esclarecer determinados hechos, aunque se negaron a instalar *Carnivore* por considerarlo innecesario.

de las conexiones a Internet, sistemas de vigilancia de las comunicaciones globales, videocámaras *online*, dispositivos de reconocimiento del rostro y escaneo de las huellas digitales) para combatir el terrorismo. Revisado durante la última semana de septiembre, culminó con su aprobación por el Senado como *Provide Appropiate Tools Required to Intercept and Obstruct Terrorism* (PATRIOT) *Act*. Incluía una nueva definición de terrorismo y contemplaba la limitación de algunos derechos fundamentales: posibilidad de intervenir las líneas de teléfono o cualquier otro dispositivo electrónico de comunicación utilizado por persona sospechosa de terrorismo, identificación de remitentes y receptores de mensajes, conducción del tráfico de los usuarios hacia servidores centrales para su control, etc. ([49]) En febrero de 2002 era enviada al Congreso una nueva propuesta de ley, la *Cyber Security and Enhancement Act*, que contenía el endurecimiento de las penas para los hackers y crackers y obligaba a los ISPs a comunicar a las autoridades la existencia de "riesgos razonables" en el tráfico de comunicaciones, y no sólo los "riesgos graves" recogidos en la *Patriot Act* ([50]).

El Reino Unido se sumó de inmediato a este tipo de regulación, con la consiguiente aprobación de normas ciertamente cuestionables ([51]). Y poco tiempo después lo haría un Land de Alemania. En el año 2006 el Estado de Renania del Norte-Wesfalia aprobó una ley que autorizaba a la policía a introducirse, a través de Internet, en los ordenadores personales de los internautas sospechosos de terro-

---

([49]) De poco sirvieron las críticas de la Unión de Libertades Civiles de América sobre la inconstitucionalidad de algunas de sus cláusulas. La norma ampliaba definitivamente el estatuto *pen register* – dispositivo de seguimiento electrónico que se conecta a una línea de teléfono y registra los números marcados – a las comunicaciones electrónicas y a la navegación por Internet, de modo que para los investigadores sería más fácil obtener los datos sobre la actividad en Internet y el registro de información privada sobre direcciones IP. También contemplaba la obligación para los proveedores de servicios de Internet de contribuir en esta intervención, permitiendo a las autoridades capturar información o facilitándola.

([50]) La exigencia de comunicar los datos de pasajeros comunitarios que utilizaran vía aérea para viajar a EE.UU. alcanzó una solución de compromiso que no satisfizo a los órganos europeos y que terminó siendo anulada por Sentencia de Tribunal de Justicia de las Comunidades Europeas de 30 de mayo de 2006 por un motivo competencial, sin entrar en el asunto de la cuestión.

([51]) En mayo de 2008 se presentó un nuevo proyecto de norma que permite la creación de base de datos, cedidos por compañías telefónicas y operadoras de Internet, sobre detalles de llamadas y correos electrónicos que serán guardados durante 12 meses, pero exige autorización judicial para que puedan ser procesados

rismo y analizar el contenido del disco duro. El 27 de febrero de 2008 se pronunciaba el Tribunal Constitucional sobre su inconstitucionalidad, dejando entrever que sólo sería constitucional tal registro si la ley lo autorizase en casos de "peligro para la vida de las personas o riesgo para el Estado", y previa autorización judicial. En su lectura pública, el Presidente del Alto Tribunal alemán recalcó que con esta sentencia se impulsaba la eficacia de un "derecho básico de garantía de confidencialidad e integridad de los sistemas técnicos de información".

En España la denuncia más notoria se ha producido sobre la red SITEL. En el año 2000 comenzó a desarrollarse un sofisticado software que permitía la interceptación de comunicaciones y la recogida de ciertos datos anexos (números y nombres de los usuarios, localización geográfica, etc.) que las operadoras debían entregar a unos "agentes facultados" antes de intervención judicial alguna. En marzo de 2004 comenzó la fase de prueba bajo riguroso control judicial, pero carecía de base legal para su utilización generalizada. El Ministerio de Industria aprobó en abril de 2005 el *Reglamento sobre las condiciones para la prestación del servicio de comunicaciones electrónicas, el servicio universal y la protección a los usuarios* (RD 424/2005, de 15 de abril) ([52]) que incluía en su articulado (artículos 88, 89, 95, 96 y 97) la interceptación de las comunicaciones sin previa autorización judicial. La Asociación de Internautas recurrió la norma ante el Tribunal Supremo por entender que suponía la restricción de derechos fundamentales (intimidad, protección de datos y secreto de las comunicaciones) y precisaba, por tanto, una regulación mediante ley orgánica.

En octubre de 2007, antes de que se produjese fallo alguno del Tribunal Supremo, fue aprobada la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*, lo que otorgaba rango legal al contenido del Reglamento recurrido. Aprobada esta ley, el Tribunal Supremo preguntó a los recurrentes sobre su desistimiento, pero éstos mantuvieron que debía ser una ley orgánica y no ordinaria la que regulara tal materia y, además, que seguía sin exigirse el control judicial previo. El 5 de febrero de 2008 el Tribunal Supremo desestimó el recurso por entender que la ley cumplía todos los requisitos exigibles al permitir simplemente la recogida de datos

([52]) El Reglamento desarrollaba la Ley 32/2003, de 3 de noviembre, *General de Telecomunicaciones*.

instrumentales sin afectar al contenido de la comunicación ([53]). En marzo de 2008 se interpuso Recurso de Amparo ante el Tribunal Constitucional alegando que el Tribunal Supremo había vulnerado el sistema de competencias al valorar la constitucionalidad de la norma sin plantear la cuestión de inconstitucionalidad al Alto Tribunal, y que la norma no respetaba las garantías previstas para los derechos fundamentales ([54]).

Es de destacar que el Tribunal Supremo ha considerado lícita la obtención de datos personales – sin previa autorización judicial – disponibles en las redes de intercambio P2P cuando es la policía quien los obtiene; así se recoge en la Sentencia 236/2008, de 9 de mayo. En ella considera que las pruebas obtenidas por la policía en este tipo de redes son válidas, porque todo lo que se puede obtener en ellas (datos, ficheros, etc.) son puestos a disposición del resto de usuarios voluntariamente por sus titulares, por lo que debe entenderse que tienen carácter público ([55]). Pero en contradicción con la sentencia de 5 de febrero anteriormente citada, entiende el Tribunal Supremo en esta posterior que las pruebas obtenidas resultan válidas porque la policía, una vez comprobados los indicios de comisión de un delito desde una determinada dirección IP, solicita autorización judicial para identificar al usuario. Este modo de proceder es el más acorde con una garantía efectiva de los derechos fundamentales, cuando se solicita la autorización judicial antes de identificar al usuario de la IP.

Desgraciadamente el riesgo que sufre nuestra privacidad no proviene solamente de instancias oficiales, sino también por parte de hackers y de empresas que desean obtener algún beneficio con los datos obtenidos. En este terreno, la primera demanda se formuló

([53]) En voto particular, uno de los Magistrados manifestaba su disconformidad con el fallo argumentando que no se garantizaba un control judicial del tipo de datos a recoger y del alcance del seguimiento (autorizados genéricamente por la ley), por lo que entendía precisa la presentación de una cuestión de inconstitucionalidad.

([54]) Aún no se ha pronunciado el Tribunal Constitucional y, dado el ritmo de resolución de los recursos, es probable que debamos esperar un par de años.

([55]) Esta sentencia anulaba otra de la Audiencia de Tarragona que consideraba nulas las pruebas obtenidas por vulnerar el derecho al secreto de las comunicaciones al "rastrear" las descargas de la usuaria denunciada sin control judicial. El Tribunal Supremo estimaba que esos rastreos se pueden llevar a cabo, dadas las características del P2P, sin violentar la privacidad de los usuarios, que consienten esa posibilidad si quieren utilizar dichos programas (no vulnera el art. 18, 1º y 3º CE). Se trata de una doctrina muy cuestionable, puesto que abre la puerta a todo tipo de abusos.

contra Netscape por obtener información – no autorizada – de los usuarios mediante su SmartDownload, programa que se activaba automáticamente al descargar archivos de la red y transmitía a Netscape información sobre la navegación para crear un perfil de descargas. Poco más tarde fue DoubleClick la demandada por procesar los hábitos de navegación de quienes usaban sus banners, mientras que Avenue A y MatchLogic lo fueron por implantar cookies en los discos duros de los internautas sin su consentimiento ([56]). La trascendencia de estas conductas se puso de manifiesto con el aumento de los mensajes electrónicos no solicitados (*spam*), que destaparon el tráfico de datos existente sin que los usuarios tuvieran conocimiento ([57]). Estas conductas, cada vez más extendidas, son constitutivas de verdaderos atentados difíciles de evitar y su fin más común suele ser la venta a otras compañías de los datos de clientes propios o de personas ajenas que han utilizado determinados servicios. Uno de los casos más relevantes en este terreno fue el de Toysmart.com, que pretendió vender las bases de datos de sus clientes antes de proceder a su cierre ([58]). En Europa – como hemos visto – la protección jurídica es mayor, aunque el problema es que muchos europeos contratan directamente con empresas norteamericanas o de otros países, que no resultan obligadas jurídicamente al respeto de las garantías europeas ([59]).

([56]) Algunos países han decidido regular restrictivamente estas prácticas, como Francia, que modificó su legislación para autorizar las *cookies* únicamente si el usuario había recibido previamente una información clara y completa sobre las finalidades del tratamiento y los medios de los que dispone para oponerse a él. Sin embargo, contempla la legalidad del uso de estos ficheros siempre que sean empleados exclusivamente para facilitar las comunicaciones, prohibiendo además que el acceso a un sitio quede condicionado a la aceptación por parte del internauta de que sus datos sean almacenados en su ordenador para otros fines que no sean los autorizados.

([57]) Véase, por ejemplo, los dictámenes del Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, en particular el Dictamen 2/2006 sobre el Respeto de la Privacidad en relación con la prestación de servicios de cribado de correo electrónico.

([58]) Tras un largo proceso, un juez federal de EE.UU. lo evitó a principios de 2001 ordenando la destrucción de la lista. Dos meses más tarde el Senado estadounidense aprobaba una ley, por 83 votos a favor y 15 en contra, prohibiendo a las compañías vender o alquilar los datos de clientes cuando para su obtención se habían comprometido a no hacerlo.

([59]) Se ha dado un gran paso en las garantías de la intimidad en la Sociedad de la Información con el reconocimiento de la dirección IP como dato de carácter personal. La dirección IP o serie de números que identifica un ordenador tiene hoy día

Fue normal también la preocupación que suscitó en ciertos círculos norteamericanos el lanzamiento de Passport por parte de Microsoft hace años. El Electronic Privacy Information Center y otras organizaciones de defensa de la privacidad presentaron el 26 de julio de 2001 una demanda formal ante la Comisión Federal de Comercio alegando que el sistema de autenticación Passport de Microsoft, incluido en Windows XP, violaba las leyes federales de "privacidad", pues obligaba a los usuarios a almacenar sus datos personales en una base de datos de la compañía. Este sistema, que recogía información personal de los consumidores – como las contraseñas e información de las tarjetas de crédito – y las almacenaba en una base para que el usuario no tuviera que reescribirlas continuamente al realizar sus compras por Internet – se introducía automáticamente –, suponía una gran comodidad para los usuarios, pero al concentrar toda la información personal de cada usuario dejaba abierta una puerta al tratamiento abusivo de los mismos, lo que suponía para los defensores de la privacidad una causa de alarma ([60]). Microsoft acudió a Washington a petición del *Center for Democracy & Technology*, grupo que defiende los intereses de los consumidores, para discutir los detalles técnicos de Passport y rebatir todas estas acusaciones.

2.1. Riesgos derivados de la protección de los derechos de autor

En la actualidad, los intentos de frenar los intercambios de contenidos digitales protegidos por derechos de autor han elevado el

---

la consideración indiscutible de dato de carácter personal porque puede revelar (no siempre) la identidad del usuario y la actividad que se desarrolla desde un ordenador. Así lo reiteró en el Parlamento Europeo (enero de 2008) Peter Scharr, Director de la Oficina de Protección de Datos alemana y presidente del Grupo de la UE que analiza los procedimientos de buscadores y titulares de otros servicios que pretenden servirse de esta información para remitir publicidad. Todos los ficheros en los que queden recopiladas estas direcciones, las direcciones de e-mail o los nombres de personas asociados a ellas – con independencia del sistema utilizado – deberán ser comunicados a las Agencias Protectoras, y su tratamiento deberá contar con el consentimiento de los afectados.

([60]) Microsoft utilizaba este sistema en MSN Messenger y en los servicios de correo electrónico de Hotmail, en el acceso online a Microsoft Developer Network y en las adquisiciones de libros electrónicos para Microsoft Reader, entre otros productos y servicios. Además, Passport también era el sistema de autenticación para HailStorm, un conjunto de servicios web que permitiría a los suscriptores acceder a sus mensajes, listas de contactos, compras y otros servicios, tales como banca o entretenimiento.

riesgo de vulneración de la privacidad. En un principio fueron generalmente las sociedades de autores las que contrataron servicios privados de software espía para identificar a los usuarios de las redes P2P que no respetaban los derechos de autor. Pero en su cruzada contra los infractores encontraron dos escollos. El primero fue el de la ilicitud de las pruebas obtenidas ilegalmente, que las invalidaba para su utilización en los procesos judiciales. El segundo, de naturaleza más grave, fue la amenaza de verse demandados por vulnerar la privacidad de los usuarios afectados por sus programas espía.

La estrategia varió al cerrarse esta puerta y el esfuerzo del mundo del cine y de la música se dirigió contra las redes P2P. Si no se podía terminar con los infractores de modo individual, el remedio podría venir de la mano de la ilegalización de las redes de pares que suministraban la tecnología necesaria. Pero perdieron también esta batalla. Los tribunales declararon que las redes P2P son idóneas también para el intercambio lícito de ficheros y resultaba excesiva, por tanto, su prohibición.

El tercer intento está ofreciendo mejores resultados. Consiste en convencer a los gobiernos de la necesidad de regular el tráfico de ficheros a través de la red, de modo que sean las operadoras que dan servicios de Internet a los usuarios quienes se encarguen de controlar el tráfico de sus clientes y eliminen la posibilidad de intercambiar contenidos protegidos por derechos de autor. Los gobiernos de Francia y Reino Unido ya han accedido a este tipo de medidas con sendos proyectos de regulación. Contemplan medidas cautelares y sancionadoras, y obligan a las operadoras a advertir a sus clientes sobre la ilicitud de su actividad, con amenaza de suspensión temporal de la conexión en caso de no cesar en los intercambios de contenidos protegidos. Una segunda advertencia conllevaría la suspensión temporal, mientras que la tercera supondría la desconexión definitiva. En el Reino Unido, fruto del acuerdo entre Virgin Media y la BPI (Industria Fonográfica Británica), comenzaron a ser enviadas las primeras misivas con advertencia de desconexión en junio de 2008.

En los países donde no se han iniciado este tipo de regulaciones, las sociedades de autores han intentado forzar a las operadoras para que entreguen los datos de tráfico y las identidades de los infractores, pero con resultado negativo. La Sentencia del Tribunal de Justicia de las Comunidades Europeas de 29 de enero de 2008, Asunto C-275/06, *Promusicae c. Telefónica de España*, ha resuelto que el derecho comunitario no obliga a los Estados a establecer una regulación similar a la proyectada por Francia y Reino Unido, porque no existe la obligación en el derecho comunitario de

facilitar los datos personales para garantizar los derechos de autor frente a infracciones civiles (sí en los casos de investigación criminal y para la salvaguardia de la seguridad pública y de la defensa nacional). En el caso de protección de derechos y libertades personales que sólo constituyen ilícitos civiles, cada Estado tiene libertad para exigir la facilitación de datos (con el principio de proporcionalidad), pero debe ser restrictivo ([61]). En el caso de España, la legislación vigente no lo permite.

No podemos ignorar que las descargas de contenidos protegidos sin autorización de los titulares de los derechos constituyen actos ilícitos y que deben ser restringidos, pero no a cualquier precio ([62]). En estos casos se confiere a las operadoras – entidades privadas – unas atribuciones excesivas que les permiten examinar y rastrear las navegaciones de sus clientes, con la consiguiente posibilidad de elaborar perfiles de su intimidad.

En el ámbito norteamericano los riesgos son más graves aún tras la sentencia de la Corte Federal del Distrito Sur de Nueva York de 1 de julio de 2008. Tras la demanda de Viacom contra YouTube (Google) por permitir el acceso a vídeos de contenidos protegidos, la citada Corte ha condenado a Google a compartir con la demandante los datos registrados de los usuarios, considerando que el conocimiento de tales datos no constituye un riesgo para la privacidad de los mismos ([63]). Sin embargo, ha denegado la segunda petición de que Google comparta su algoritmo de búsqueda y su código fuente a fin de impedir técnicamente nuevas infracciones. El argumento del juez es que esto supondría un riesgo para los secretos empresariales, mostrando así la escasa atención que presta el derecho norteamericano a la salvaguarda de la privacidad en comparación con el europeo ([64]).

([61]) Véase Sentencia del Tribunal de Justicia (Gran Sala) de 29 de enero de 2008, Asunto C-275/06, *Productores de Música de España (Promusicae) y Telefónica de España, S.A.U.*, en *RCE* 90/2008, 91-112.

([62]) Véase, sobre esta cuestión, J.J. Megías Quirós, *Hacia una propiedad intelectual comunitarista*, en *Sociedad de la Información: Derecho, Libertad, Comunidad*, cit., 121-209.

([63]) Incluso Viacom está convencida de que esos datos pueden vulnerar la privacidad, por ello pretendió negociar con Google el modo de que le fueran facilitados los datos con garantías para los usuarios, alegando que sólo quería mostrar en los tribunales el daño que sufría en sus contenidos protegidos.

([64]) Esta es la razón de que en reiteradas ocasiones los organismos de protección europeos hayan denunciado las escasas garantías que ofrece el derecho nor-

2.2. Los riesgos de la privacidad en el ámbito laboral

La implementación de los medios tecnológicos en el ámbito laboral ha dado lugar a numerosos conflictos jurídicos entre empleados y empleadores por los riesgos que conllevan para la intimidad y el secreto de las comunicaciones. No es de extrañar, por ello, que hayan debido pronunciarse al respecto en reiteradas ocasiones tanto los tribunales como los órganos encargados de velar por la protección de datos de los trabajadores. El Garante para la Protección de los Datos Personales de Italia aprobó el 1 de marzo de 2007 una instrucción sobre utilización del correo electrónico e Internet en el marco de la relación de trabajo. En ella se excluía la posibilidad de lectura y registro sistemático de los mensajes electrónicos, así como la de recabar información sobre éstos salvo en lo necesario para el buen funcionamiento del servicio. Igual tratamiento recibía la navegación en Internet de los empleados. Varios meses más tarde se pronunció en términos similares la Agencia Española de Protección de Datos en su Informe Jurídico 0391/2007 sobre *Cribado de correo electrónico*.

El control del correo electrónico, de la navegación por Internet y de la utilización de los ordenadores se ha convertido en uno de los supuestos más repetidos de injerencia por parte del empresario, público o privado, en la privacidad de los empleados ([65]). A ello se debe que contemos ya con la primera sentencia del Tribunal Europeo de Derechos Humanos, dictada el 3 de abril de 2007 en el asunto *L. Copland c. Reino Unido*. Durante seis meses se había controlado el teléfono, el correo electrónico (direcciones, fechas y horas de envío de mensajes) y la navegación por Internet (páginas visitadas, fecha, hora y duración) de una trabajadora de un College público sin su conocimiento, sin autorización judicial y sin base legal alguna que permitiera tal control ([66]). La doctrina sentada por el Tribunal es clara:

---

teamericano. En este sentido se pronunció de nuevo la Agencia Española de Protección de Datos en su Informe Jurídico 0391/2007, sobre Cribado de Correo Electrónico, al afirmar expresamente que Estados Unidos "no ofrece un nivel adecuado de protección" (4).

([65]) Véase M. RODRÍGUEZ-PIÑERO, J.L. LÁZARO, *Los derechos on-line en el ordenamiento laboral español: estado de la cuestión*, en *Derecho y Conocimiento*, 2/2003, 151-173; S. RODRÍGUEZ ESCANCIANO, *La potencialidad lesiva de la informática sobre los derechos de los trabajadores*, en *Revista Española de Protección de Datos*, 2/2007, 95-158.

([66]) El Gobierno británico alegó tras la demanda que no se había llegado a interceptar las llamadas, ni a analizar el contenido de las páginas, ni el de los correos

a) Toda comunicación efectuada desde el centro de trabajo quedan incluidas en el concepto de "vida privada", ya sea telefónica, electrónica o de navegación en Internet ([67]);

b) la inexistencia de advertencia previa del control induce al trabajador a confiar en la privacidad de sus acciones ([68]);

c) la información relativa a la fecha y duración de las conversaciones telefónicas y de los números marcados forman parte de las comunicaciones y, aunque se hayan conseguido estos datos legítimamente (a través de facturas), su conocimiento constituye una injerencia en la vida privada ([69]);

d) la ley puede regular la posibilidad del control y seguimiento con fines legítimos, pero el vacío legal no puede dejar al trabajador a merced del control indiscriminado del empresario ([70]).

"En consecuencia, el Tribunal considera que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por Internet de la demandante, sin su conocimiento, constituye una injerencia en su

---

y que sólo pretendía realizar un análisis para comprobar si se hacía un uso personal de los medios del College; entendía que no se trataba de una injerencia en la vida privada y que, aun constituyéndolo, estaría justificada por constituir una medida proporcionada para preservar un interés (fondos) público. La demandante dudaba que no se hubieran leído sus correos y alegaba, además, que el College carecía de legitimidad para vigilar a los trabajadores y que lo había efectuado con medios innecesarios y desproporcionados.

([67]) Sentencia Copland, núm. 41: "Según reiterada jurisprudencia del Tribunal, las llamadas telefónicas que proceden de locales profesionales pueden incluirse en los conceptos de 'vida privada' y de 'correspondencia' a efectos del artículo 8.1 (…) Es lógico pues que los correos electrónicos enviados desde el lugar de trabajo estén protegidos en virtud del artículo 8, como debe estarlo la información derivada del seguimiento del uso personal de Internet".

([68]) En el número 42 especifica que no se advirtió a la demandante del control de su actividad, por lo que "podía razonablemente esperar que se reconociera el carácter privado" de sus llamadas, su correo y su navegación.

([69]) Cfr. Sentencia Copland, núm. 43. Habría que incluir las direcciones electrónicas y también los datos relativos a los correos.

([70]) "El Tribunal no excluye que el seguimiento del uso por parte de un trabajador del teléfono, el correo electrónico e Internet en el lugar de trabajo pueda considerarse 'necesario en una sociedad democrática' en ciertas situaciones que persigan un fin legítimo", pero debe estar regulado explícitamente para evitar la arbitrariedad. Cfr. Sentencia Copland, núm. 48.

derecho al respeto de su vida privada y su correspondencia, en el sentido del artículo 8 del Convenio" ([71]).

La jurisprudencia del Tribunal Constitucional español también ha fijado algunos principios básicos a la hora de enjuiciar este control. La Sentencia 281/2005, de 7 de noviembre, reconocía el poder de la empresa sobre los ordenadores de su propiedad, pero sin un carácter "omnímodo e indiscriminado", careciendo de una "libérrima facultad de control de su contenido, haya o no documentos personales". Por su parte, en las Sentencias 98/2000, de 10 de abril, y 186/2000, de 10 de julio, se reconoce al trabajador en el desempeño de su trabajo un "ámbito propio y reservado frente a la acción y conocimiento de los demás", incluido el empresario; es cierto que no se trata de un derecho absoluto y que puede, por tanto, ceder ante intereses constitucionalmente relevantes, pero para ello se exige la conclusión satisfactoria de tres juicios conjuntamente: *a*) *de idoneidad*: que con tal medida se pueda lograr el objetivo propuesto; *b*) *de necesidad*: que no exista otra medida más moderada para lograr el mismo objetivo con igual eficacia; y *c*) *de proporcionalidad*, esto es, que la medida sea ponderada y equilibrada, de modo que deriven de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto ([72]).

El ordenamiento laboral español contiene unos preceptos en el Estatuto de los Trabajadores (ET) que permiten al empresario dos tipos de control sobre sus empleados y los bienes materiales. Uno de ellos es el artículo 20.3, que permite a la empresa adoptar las medidas oportunas para controlar y vigilar el cumplimiento de las obligaciones laborales por parte de sus trabajadores, así como el control de los bienes de la empresa. Se trata de un "poder ordinario" o normal, limitado por el respeto de la dignidad e intimidad de los trabajadores, como establece el artículo 4.2 del mismo texto legal. El otro precepto significativo es el artículo 18, que otorga un "poder extraordinario" de control que permite el registro sobre la persona del trabajador, así como el registro de sus taquillas y efectos personales; para su ejercicio se precisa contar con una razón que lo justifique – que puede ser perfectamente la protección del patrimonio empresa-

([71]) Sentencia Copland, núm. 44. Más adelante (núm. 54) da a entender que la injerencia hubiera sido más grave si hubiera interceptado las llamadas, conocido el contenido de los correos o analizado el contenido de las páginas visitadas, pero el hecho de no hacerlo no convierte el seguimiento en lícito, simplemente es menos grave.

([72]) Cfr. STC 186/2000, Fundamento Jurídico 6º.

rial y del resto de los trabajadores – y que se efectúe en presencia de un representante de los trabajadores.

Este artículo 18 ET había servido a los tribunales españoles para resolver los primeros supuestos planteados. Así lo entendieron el Tribunal Superior de Justicia de Andalucía ([73]), de Galicia ([74]) y del País Vasco ([75]). Coincidían en que de no existir normas ni advertencia expresa sobre la prohibición absoluta de uso con fines personales, los registros del ordenador sin consentimiento del trabajador, sin autorización judicial o sin presencia de un representante y razón justificada constituyen una clara vulneración de la vida privada.

El recurso para unificación de doctrina presentado contra la Sentencia del Tribunal Superior de Justicia de Galicia de 25 de enero de 2006 ha dado lugar a la Sentencia del Tribunal Supremo 8807/2007, de 26 de septiembre. El motivo de litigio era el despido de un trabajador por utilizar el ordenador de la empresa para acceder a páginas pornográficas, lo que ocasionó la contaminación por virus del sistema; el efecto de los virus hizo que la empresa solicitara a los técnicos su reparación, en cuyo transcurso se registró el contenido del ordenador en presencia del Administrador (no del trabajador ni de representante sindical), haciendo copia de los archivos temporales antiguos que demostraban el acceso a las citadas páginas. Reparado el ordenador, se repitió veinte días más tarde la operación de registro y copia en presencia de dos delegados de personal, pero ausente el trabajador y sin su consentimiento.

El Tribunal Supremo recoge en esta sentencia los argumentos del Tribunal Europeo de Derechos Humanos en el Asunto Copland, advirtiendo que – siendo lícito un cierto control – el conflicto puede derivar de las "dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador (…) y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa" que sirven para cumplir la prestación laboral; pero a diferencia de los Tribunales Superiores anteriormente citados, entiende que tal control quedaría "dentro del ámbito del

([73]) La Sala de lo Social (Málaga) del Tribunal Superior de Justicia de Andalucía, en su Sentencia de 25 de febrero de 2000.

([74]) Sentencia de 25 de enero de 2006.

([75]) Sentencias de 21 de diciembre de 2004 y de 12 de septiembre de 2006.

poder (ordinario) de vigilancia del empresario" (artículo 20.3 ET) siempre que se respete la dignidad del trabajador ([76]).

En contra de la doctrina mayoritaria y de la jurisprudencia producida hasta la fecha, entiende que el artículo 18 ET no es aplicable a los medios informáticos facilitados por la empresa para la ejecución de la prestación laboral, porque en los registros de taquillas y efectos personales de los trabajadores amparados por este artículo, el empresario actúa de forma excepcional como "policía empresarial" y al margen de lo que le permite el marco contractual. Entiende que "las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes (de control): el ordenador es un instrumento de producción del que es titular el empresario 'como propietario o por otro título' y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen" ([77]). Viene a afirmar, por tanto, que el hecho de que se ejecute la prestación de trabajo con el ordenador habilita al empresario para verificar en él su correcto cumplimiento, y se trata de un control normal de los medios de producción.

En mi opinión, tal criterio no debería ser aplicable a los medios informáticos puestos a disposición de los trabajadores, pues estos son idóneos para guardar documentos, fotos, vídeos, etc., en los que estén muy presentes rasgos y datos que aporten información muy sensible relacionada con la ideología, religión, moral, orientación sexual, etc. que pertenecen al ámbito de la privacidad del usuario. La presencia de un representante constituye un medio indirecto añadido de preservar la intimidad, de modo que el empresario no pueda actuar indiscriminada y arbitrariamente. En una máquina de hacer tornillos no puede reflejarse la intimidad del trabajador, en un ordenador sí, por muy de la empresa que sea, de modo que la presencia del representante añade un plus que garantiza de modo más real el respeto de los derechos fundamentales. Tal presencia no constituye una simple garantía de objetividad de la prueba, como mantiene el Tribunal Supremo, garantía que se puede alcanzar por otras vías – como la grabación del registro, por ejemplo –, sino que le somete a

([76]) Cfr. Fundamento Jurídico 2º. En el mismo sentido, cfr. Informe Jurídico 0391/2007 de la Agencia Española de Protección de Datos sobre *Cribado de correo electrónico*, cit., 6-7.

([77]) Fundamento Jurídico 3º.

otra opinión sobre la proporcionalidad y control de legalidad de lo que se va a llevar a efecto sin una previa autorización judicial.

En definitiva, los criterios fijados por el Tribunal Supremo son los siguientes:

1º El poder de control que corresponde al empresario sobre el uso del ordenador por parte de los trabajadores debe ser considerado como el control normal y similar al que puede realizarse sobre cualquier otro bien de producción, sin requerir garantías especiales como pudiera ser la presencia de representantes sindicales.

2º Tal poder sólo está limitado por el respeto de la dignidad e intimidad de los trabajadores, que carecen de carácter absoluto y no excluyen todo control ([78]).

3º El empresario debe fijar claramente unas normas de uso del ordenador y del acceso a Internet, que pueden excluir cualquier uso personal ([79]). Tales normas deben explicitar los medios de control que serán efectuados ([80]).

4º Si no existen tales normas, debe presumirse que existe autorización para una utilización personal moderada, siendo preci-

---

([78]) Debe respetar la intimidad en los términos dictados por el Tribunal Constitucional en sus Sentencias 98 y 186/2000, teniendo en cuenta "el hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores", lo que crea "una expectativa también general de confidencialidad en esos usos". Dicha expectativa no puede ser desconocida, pero tampoco convertirse en causa de exclusión absoluta de control si se han establecido instrucciones para su uso y controles para verificar la correcta utilización que garantice la permanencia del servicio. Cfr. Fundamento Jurídico 4º.

([79]) Los límites que puedan establecer estas normas dependerán del empresario o de la negociación con sus trabajadores, pero pueden ser exhaustivos. Puede servir de ejemplo la Instrucción 2/2003, de 26 de febrero, del Pleno del Consejo General del Poder Judicial de España, que en su artículo 9 impone a todos los usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia – incluidos los magistrados – la prohibición de utilizar el "correo electrónico para actividades personales restringidas en las que pueda haber alguna expectativa de privacidad o secreto en las comunicaciones".

([80]) "Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios – con aplicación de prohibiciones absolutas o parciales – e informar a los trabajadores de que va a existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos (…). De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizar el control, se ha vulnerado 'una expectativa razonable de intimidad' en los términos que establece el Tribunal Europeo de Derechos Humanos en las Sentencias *Halford* y *Copland*" (Fundamento Jurídico 4º).

so en estos casos el consentimiento del trabajador o la previa autorización judicial para efectuar el registro ([81]).

En mi opinión, estos criterios conllevan una disminución de las garantías legales de derechos tan importantes como la intimidad y el secreto de las comunicaciones del trabajador. Nadie pone en duda que el ordenador es propiedad de la empresa y que puede ser esencial para la producción, pero igual de evidente es que constituye una herramienta peculiar en la que puede quedar reflejada con gran facilidad información íntima del usuario, lo que requiere un tratamiento distinto al resto de las herramientas profesionales. Creo que, existiendo o no normas de uso, es preciso excluir cualquier control indiscriminado y arbitrario del empresario o directivos ([82]), lo que podría lograrse con la necesidad de aportar una razón justificada para llevarlo a cabo y la presencia de un representante del trabajador, como exige el citado artículo 18 ET. En el asunto Copland, el Tribunal Europeo de Derechos Humanos no pudo entrar en esta cuestión porque el Reino Unido carecía de regulación similar, pero considero que la regulación laboral española es más respetuosa con la intimidad y sería preciso aprovecharla como un plus en la garantía de los derechos humanos ([83]).

Por otra parte, considero también necesario establecer una clara diferencia entre el simple control del ordenador y el control

---

([81]) En el supuesto enjuiciado entendió vulnerada la intimidad del trabajador por proceder al registro sin que existieran normas previas que prohibieran el uso personal. Cfr. Fundamento Jurídico 5º.

([82]) La ya citada STC 98/2000, de 10 de abril, establece que la relación laboral no supone una renuncia absoluta a la intimidad, siendo necesario en cada caso concreto valorar si las medidas de vigilancia y control establecidas pueden dañar el derecho a la intimidad de los trabajadores. En su Fundamento Jurídico 6º concreta esta valoración en "si la instalación se hace o no indiscriminada y masivamente, si los sistemas son visibles o han sido instalados subrepticiamente, la finalidad real perseguida con la instalación de tales sistemas, si existen razones de seguridad, por el tipo de actividad que se desarrolla en el centro de trabajo de que se trate, que justifique la implantación de tales medios de control, etc.".

([83]) Esta es la impresión que se obtiene a partir de los documentos elaborados en el seno de la Unión Europea por el *Grupo del Artículo 29* (Recomendación 1/2001 sobre datos de evaluación de los trabajadores, Dictamen 8/2001 sobre tratamiento de datos personales en el contexto laboral, Documento de Trabajo de 29 de mayo de 2002, relativo a la vigilancia por parte del empleador de la utilización del correo electrónico e Internet por parte de los trabajadores y Dictamen 2/2006 sobre el Respeto de la Privacidad en relación con la prestación de servicios de cribado de correo electrónico) y por el *Grupo Berlín* (Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales).

del contenido de los correos electrónicos, pues en este último supuesto no sólo queda afectada la intimidad, sino también el secreto de las comunicaciones con todas sus características peculiares. Los mensajes electrónicos de los empleados (recibidos o enviados) desde sus puestos de trabajo y en horario laboral pueden contener referencias íntimas del trabajador e, incluso, de terceros sin relación alguna con el entorno laboral. Es cierto que el trabajador no tiene reconocido un derecho universal a usar de forma privada los medios tecnológicos que la empresa pone a su disposición para el desempeño de su cometido laboral, pero tampoco se le prohíbe expresamente. La solución definitiva, como han reiterado todos los tribunales, tendrá que venir de la mano de una nueva regulación legal que se enfrente a este problema, pero mientras tanto debe ser la negociación colectiva o los empleados y empresarios, en particular, los que tengan que pactar unas medidas concretas. La doctrina mayoritaria entiende, al igual que la jurisprudencia – como ya hemos visto –, que las medidas de control son lícitas cuando existe una política clara de la empresa, estableciéndose un código de conducta conocido por los trabajadores y unas reglas accesibles y admitidas por éstos. Por tanto, habría que descartar a priori que sea lícita cualquier medida de control sin más como facultad del "poder normal" del empresario.

Además, habría que distinguir entre el uso de una dirección personal desde el puesto de trabajo (minombre@miservidor.com) y el uso de una dirección particular creada para el trabajo (minombre@empresa.com) o el uso de una dirección creada con fines exclusivamente profesionales (departamentodeempresa@empresa.com). En el primer supuesto nos encontraríamos ante un posible uso indebido del acceso durante el horario laboral; la cuenta de correo será intocable por parte de la empresa. Equivale a la carta privada que recibe un trabajador en su lugar de trabajo y que dejan sobre su mesa al repartir el correo, por lo que nadie tiene derecho, ni siquiera el empresario, a abrir esa correspondencia; el simple hecho de utilizar identificadores privados hace presumir que el trabajador lo utiliza para fines privados.

En el segundo supuesto resulta afectado el nombre de la empresa, por lo que se deben fijar unas reglas de uso – mejor pactadas – y, en caso de indicio de uso inadecuado, el control del contenido deberá motivarse y requerirse autorización judicial o consentimiento del usuario. La propiedad del ordenador y la titularidad sobre la dirección electrónica no faculta al empresario a un control indiscriminado de su uso, no tanto por una vulneración de la intimi-

dad (más complicado en el ámbito laboral) ([84]), sino por el derecho al secreto de las comunicaciones (garantía formal) y por mermar la libertad de autodeterminación y la dignidad en el trabajo. El Código Penal español también ampara el derecho al secreto de las comunicaciones en el trabajo, y el art. 197 sería plenamente aplicable ([85]). Así como el derecho a la intimidad en el trabajo admite limitaciones, también el derecho al secreto de las comunicaciones las puede admitir, aunque se deben excluir las conductas arbitrarias por parte del empresario ([86]). Esta ha sido la doctrina establecida por la Sala de lo Penal del Tribunal Supremo en sus Sentencias 666/2006, de 19 de junio, y 358/2007, de 30 de abril. Esta última resuelve el recurso de Casación interpuesto por un trabajador municipal que entendía vulnerada su intimidad y el secreto de sus comunicaciones al ser copiado uno de sus correos electrónicos durante una prolongada baja laboral. El Tribunal Supremo entiende que cuando el ordenador es de titularidad de la empresa o de la Administración y la cuenta electrónica tiene como fin el desempeño de las funciones laborales, ante

---

([84]) Afirma el Tribunal Constitucional en su Sentencia 186/2000, de 10 de julio, Fundamento Jurídico 6º, que "también hemos afirmado que el atributo más importante del derecho a la intimidad, como núcleo central de la personalidad, es la facultad de exclusión de los demás, de abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusiva, como a la divulgación ilegítima de esos datos. La conexión de la intimidad con la libertad y dignidad de la persona implica que la esfera de la inviolabilidad de la persona frente a injerencias externas, el ámbito personal y familiar, sólo en ocasiones tenga proyección hacia el exterior, por lo que no comprende, en principio los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la actividad laboral, que están más allá del ámbito del espacio de intimidad personal y familiar sustraído a intromisiones extrañas por formar parte del ámbito de la vida privada". Con todo, hay que decir que el derecho a la intimidad "en principio" queda excluido del ámbito laboral, pero no definitivamente; y lo mismo ocurre con el derecho al secreto de las comunicaciones. El trabajador no pierde estos derechos mientras realiza su trabajo, aunque pueden resultar limitados por exigencias de las circunstancias.

([85]) Sobre las consecuencias penales, véase C.Mª ROMEO CASABONA, *La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet*, en *Derecho y Conocimiento*, 2/2003, 123-149.

([86]) Afecta no sólo al conocimiento directo del contenido de los mensajes, sino también al conocimiento indirecto que pueda derivar de los filtrados. Así lo expone la Agencia Española de Protección de Datos en el citado informe sobre cribado de correo electrónico cuando afirma que "existe legitimación para filtrar el contenido del correo electrónico de los empleados, pero siempre que se trate de una cuenta de correos proporcionada por la empresa para el desarrollo de sus funciones laborales y siempre que se haya informado previamente a los trabajadores sobre dicho filtrado y los medios que se van a utilizar" (6). Véase también su informe de 10 de abril de 2006.

una baja laboral y la necesidad de continuar con el normal desarrollo de las prestaciones de la empresa hacia sus clientes, es lícito abrir el correo si esta es la única vía de cumplir con las obligaciones adquiridas por la empresa o por la entidad pública implicada[87]. En ningún momento admite que tales circunstancias justifiquen el visionado de todos los correos electrónicos recibidos o enviados, sino el de aquellos que tengan como objeto el desarrollo de las normales prestaciones laborales. Por ello afirma el tribunal Supremo que "se podrían haber planteado cuestiones distintas en el caso de que, aun cuando no fuera previsible el hallazgo de datos reservados o íntimos, tal hallazgo se hubiera producido, pues en ese caso sería valorable la reacción de los autores ante tal suceso" ([88]).

El último tipo de cuenta de correo (empresa@empresa.es) es el más claro de todos, pues lo que hace el trabajador es operar en nombre de la empresa con una dirección electrónica de ésta, por ello debe excluirse el uso personal; la empresa podría controlar perfectamente el contenido y abrir los mensajes sin necesidad del consentimiento de ninguno de los empleados que tengan acceso a la misma ([89]). Pensemos, por ejemplo, que una enfermedad del trabajador que normalmente opera con esa dirección de correo podría dejar inoperantes los servicios de pedidos, atención al cliente, servicio técnico, etc.

([87]) Se trataba de un ordenador de titularidad pública – utilizado en ocasiones por otros trabajadores – y una cuenta de correo electrónico para el desempeño del trabajo, de cuya apertura se obtuvo el documento de naturaleza pública buscado e imposible de conseguir por otras vías dada la enfermedad del trabajador. Por ello afirma el Tribunal Supremo que "no es posible afirmar que la voluntad de los acusados estuviera caracterizada por la finalidad de vulnerar la intimidad del recurrente, pues razonablemente solo era posible esperar el hallazgo de datos públicos en los archivos revisados. Ello coincide además con la conducta posterior de aquellos una vez accedieron al ordenador, pues exclusivamente utilizaron un mensaje de correo electrónico con las características expuestas en el hecho probado, que excluye en su contenido tanto la naturaleza de datos íntimos como la de datos reservados, en cuanto que se trataba de un reenvío procedente de la Alcaldía de un mensaje que previamente había sido remitido precisamente al Alcalde, y relacionado con un borrador de un convenio urbanístico. Es decir, exclusivamente en relación con actuaciones administrativas de los órganos municipales". STS 358/2007, de 30 de abril, Fundamento Jurídico 1º.

([88]) STS 358/2007, de 30 de abril, Fundamento Jurídico 1º, último párrafo.

([89]) En este último caso se podría ejercer todo tipo de control, tanto el formal (número de envíos, duración, destinatarios, tipo de archivos, etc.) como el material (propiamente del contenido, con apertura de los mensajes y ficheros).

3. *Conclusión*

Corresponde a los legisladores y a los jueces la obligación de habilitar los mecanismos y vías necesarias para que la protección de la privacidad no tenga que discurrir por los senderos propios del mercantilismo, es decir, de recurrir al derecho de propiedad sobre lo íntimo y sobre los datos para obtener una garantía efectiva. Es preciso otorgar unos mecanismos propios y adecuados en la Sociedad de la Información, complementados por la autorregulación, pero sin dejar todo en manos de ésta con el peligro del sometimiento a los más fuertes (las grandes empresas). La tarea no es sencilla porque los Estados suelen apelar continuamente a la seguridad nacional para establecer limitaciones excesivas, facultando incluso a entidades privadas que le faciliten la labor mediante el almacenamiento de datos y su procesamiento posterior. Por ello, y en este sentido se inclinan los altos tribunales, precisamos normas que establezcan de modo claro los fines que persiguen los bancos de datos autorizados y las limitaciones incuestionables. Precisamos normas que establezcan unas exigencias mayores en torno al consentimiento otorgado por los usuarios sobre sus datos, exigencias que contemplen una mayor claridad en cuanto a su recolección – en cláusulas contractuales en lugar preeminente, por ejemplo – y en cuanto a su destino. Precisamos normas que eliminen los conceptos abstractos que den pie a interpretaciones ambiguas. Precisamos normas que excluyan el tratamiento de información personal sensible, aunque técnicamente sea posible. Y precisamos normas que tengan un carácter dinámico, capaces de adaptarse a la variabilidad propia de la Sociedad de la Información. Sólo así podremos asegurar la transparencia que exige la estructura de una sociedad verdaderamente democrática.